

YOUTH SERVICES POLICY

Title: Internet and Email Usage Next Annual Review Date: 11/12/2010	Type: A. Administrative Sub Type: 5. Information Services Number: A.5.6
	Page 1 of 4
References: Office of Information (OIT) Technology Standard IT STD-005 (Personal Computing: Browser/Viewer/Plug-Ins) and OIT Policy IT-POL-013	
STATUS: Approved	
Approved By: Mary L. Livers, Deputy Secretary	Date of Approval: 11/12/2009

I. AUTHORITY:

Deputy Secretary of Youth Services as contained in La. R.S. 36:405. Deviation from this policy must be approved by the Deputy Secretary.

II. PURPOSE:

To establish the Deputy Secretary's policy regarding state-provided Internet and email usage.

III. APPLICABILITY:

All employees of Youth Services (YS), as well as contract personnel whose access to or use of Internet or email services is funded by YS or is available through equipment owned or leased by YS. Each Unit Head is responsible for ensuring that all necessary procedures are in place to comply with the provisions of this policy.

IV. DEFINITIONS:

Access - to program, to execute programs on, to communicate with, store data in, retrieve data from, or otherwise make use of any resources, including data or programs, of a computer, computer system, or computer network.

Computer Equipment - includes computer file servers, desktop/notebook computers, data communications equipment, personal digital assistants (PDA) and Blackberries .

Unauthorized Email Access - ability to view, send, receive, modify, delete, print, or copy an email where the individual gaining access does not have the right or the need to access the email.

Unauthorized Internet Activities - accessing web sites for non YS-related purposes. Also included is downloading of information, files and/or programming using file transport protocol (FTP) or any other downloading of utilities.

Unauthorized Internet Use - access to the Internet where the individual gaining access does not have the right or the need to use the Internet. This includes access and unauthorized viewing of web-based data files that include youth information.

Unit Head - Deputy Secretary, Facility Directors and Regional Managers.

YS Central Office - Offices of the Deputy Secretary, Undersecretary, Chief of Operations, Assistant Secretary, Deputy Assistant Secretaries, Deputy Undersecretary and their support staff.

V. POLICY:

It is the Deputy Secretary's policy that access to the Internet and email capabilities enhances productivity, staff communication, and the business functions of Youth Services. Internet and email usage shall be for official business only. Brief, incidental use of the Internet not on a recurring or regular basis and not related to personal business is permitted.

Access to pornographic or similar Internet web sites and all other similar uses are strictly prohibited at all times. Users may not download, transmit, display, or store any image or document using the agency system or resource that violates federal, state, or local laws and regulations, executive orders, procedures, standards, or guidelines. An abuse of the privilege of Internet or email use may result in disciplinary action.

All employees having Internet and email capabilities are responsible for preventing unauthorized access, including remote access to individual, password-protected email accounts by nonemployees or other unauthorized individuals.

Computer virus software with the latest virus subscription updates must be installed on all computers that have Internet and/or email capabilities.

VI. INTERNET APPROVAL PROCEDURES:

- A. An employee may request internet access by completing the Request for Internet Access form [Attachment A.5.6 (a)] and submitting the form to the Unit Head.
- B. The Unit Head is responsible for approving the employee's request and submitting the completed form to the I/T Director at YS Central Office.
- C. The I/T Director will provide final authorization and ensure that the employee receives the appropriate level of internet access.

VII. INTERNET PROCEDURES:

- A. Internet access is granted only to employees who need access to perform their job duties. Because of the agency use of email as a communication mechanism, restrictions on Internet or email accounts are determined by the Unit Head.

Two levels of Internet access are available. One level is very restrictive, limiting employees to a small number of web sites. Additional sites can be added at the request of the Unit Head. This very restrictive level is appropriate for employees who need access to information only available via the web, such as the ISIS Human Resources help site for timekeepers. The second level of Internet access is less restrictive and provides more flexibility for those employees needing broader access to the Internet.

- B. Microsoft Internet Explorer, the State's standard web browser, will be used for accessing web sites and services. All Internet usage will be routed through the YS computer network. Access to personal web sites and services are automatically blocked (i.e. gmail and hotmail and yahoo, facebook, my space, etc.). All Internet usage is tracked and any questionable usage will be reported by IT to the Deputy Secretary for disposition.
- C. YS will have one official web site (www.ojj.la.gov.) This web site can include links to individual unit web sites. All information posted on the web site must have prior approval from the Undersecretary or the Undersecretary's designee at the Central Office. Web content may be any information that is clearly identified as public record. Web sites shall be designed to operate on both high-speed and low-speed Internet connections.

VIII. EMAIL PROCEDURES:

- A. All emails will be sent and received using a YS approved email system.
- B. All emails sent to or received by YS employees will be scanned for computer viruses by the YS computer system. The system will reject emails detected with a computer virus. Email attachments received from outside individuals should not be opened or detached unless it is from a known and trusted source. Such attachments may contain computer viruses.
- C. Email is not designed for long-term document storage. Each employee will have an electronic mailbox with limited data storage. Emails that must be retained long-term may be archived to the employee's computer using the archiving feature.
- D. Any emails that can be considered part of the unit's records retention schedule should be printed and a hard copy retained in the appropriate file.
- E. Employees are responsible for the content of their emails. Because emails are not encrypted, there should be no expectation of confidentiality or privacy. All email is subject to monitoring and auditing.

Previous Regulation/Policy Number: A.5.6

Previous Effective Date: 08/14/08



Attachments/References: A.5.6 (a) Request for Internet Access 11-09.doc